REMARKS

Claims 1-16 are pending in the application. Claims 1 and 4-16 have been amended. Reconsideration of this application is respectfully requested.

Claims 1 and 4-16 have been amended to eliminate reference numbers.

The Office Action rejects claims 9-12 under the second paragraph of 35 U.S.C. 112 as indefinite because of antecedent issues. Claims 9-11 have been amended to depend from claim 5 so as to have antecedent basis for "the step of selecting a virus-free certificate authority referring to a first table". Claims 9 and 10 have also been amended in their second bulleted items to read "according to a list of one or a plurality of anti-virus programs that is included in the virus-free certificate". Claim 12 has been amended to depend from claim 10. I t is submitted that these amendments make claims 9-12 fully compliant with the second paragraph of 35 U.S.C. 112. Accordingly, it is submitted that the rejection of claims 9-12 under the second paragraph of 35 U.S.C. 112 is obviated by the amendment.

The Office Action rejects claims 1 and 13-16 under 35 U.S.C 103(a) as unpatentable over U.S. Patent No. 6,233,577 to Ramasubramani et al., hereafter Ramasubramani, in view of U.S Patent No. 6,347,398 to Parthasarathy et al., hereafter Parthasarathy.

The object of Ramasubramani is to provide certificates to thin client devices. These client devices are owned by users. Certificates are issued but undesignated (column 7, lines 38-40). They are stored in a local database managed by a local manager (Certificate Manager Module - CMM). Free certificates are always available. There is a process to get a batch of new certificates when it is necessary.

The present invention is not directed to certificates for users or devices but is related to file certificates. A file certificate certifies that a file is virus-free. Requests for certificates are not sent by thin clients, but by any device in the network. A request is not for a device but for a file stored (or in standby) in a network device. A certificate can only be filled by a server, so the proxy doesn't have a set of free certificates to fill for answering a request. Depending on whether the file is known or not, the following actions are performed:

- if the Virus-free Certificate Authority (VCA) knows the file, in this case the certificate is ready,
- if the VCA doesn't know the file, the file is checked using anti-virus programs.

There is no batch mode to get new free certificates. There is no free certificate. A request is sent to the VCA for each file. In a particular embodiment, the request is dispatched by the proxy to the most appropriate VCA.

In Ramasubramani, no information related to the requester is forwarded to the Certificate Authority (CA) while in the present invention, all file identifiers are forwarded to the CA.

Ramasubramani stores certificates. These certificates are only free certificates. In the present invention, the proxy doesn't store any certificate - free or filed - but just acts as a relay between the requester and the VCA.

The object of Parthasarathy is to download software from a computer network and to verify said software. The present invention is not designed to download software from such computer networks but to work on files already located in network devices. According to the present invention, for such files, requests are intercepted and forwarded to the VCA. Requests include file identifiers. A file identifier may include the file itself. In the VCA, the file is checked and a certificate is provided. The certificate is downloaded, but not the

file because the file is already located on the requesting device. The present invention cannot be compared with Parthasarathy. Parthasarathy downloads files. In the present invention, only a file upload to the VCA is optionally performed. The file in the VCA is then discarded.

In Parthasarathy, a mechanism provides a signature of the file. This signature may be incorporated in the certificate joined to the file. That doesn't mean that the file is virus free, but means that the author of the file has generated a signature when the file has been created thinking that his/her computer was virus-free at this time. There is no indication in the certificate (or even outside the certificate in any transmitted information) concerning the virus checker program used and its level. The trust about this "file safe" information is therefore very limited. In general, signatures of files are generated by the authors. However, no trust can be given to these authors since they may be hackers. Only an independent organization for checking and providing virus-free certificates can be trusted. A certificate is always valid by itself but the problem is to trust the Certificate Authority that has issued the certificate. The present invention can include a signature similar to the one used in Parthasarathy. The problem is that the signature is just one of the identification parameters incorporated in the virus-free certificate. The object of the present invention is to avoid the use of information provided by the author of the file. The signature used in the present invention is based on keys provided by a trusted CA and not on keys used by the author to generate its own file signature. Compared with Parthasarathy, the file signature is different in the present invention.

Parthasarathy neither teaches nor suggests the fact that a digital certificate can include more that just a file signature. A legacy file or a device certificate always contains a signature so the incorporation of a file signature in a digital certificate is not new. For some people a signature is sufficient to believe that a file is virus-free. That is not what Applicants believe. That is the reason why the virus-free digital certificates according to the present invention contain

many more fields. Applicants cannot find in Parthasarathy this plurality of fields in addition to the file signature. Furthermore, there is a lack of description of the certificate structure in Parthasarathy. The process to tell that the file is safe and virus-free is not explained. Also, the following questions are not discussed in Parthasarathy: where keys are coming from, what kind of checking is performed, what is the validity, and which CA is used.

In Parthasarathy, the file certificate is issued by the author of the file (column 8, line 43). Trusting a person that says that the file is safe (column 8 line 41) with no arguments is particularly difficult and risky.

With respect to independent claims 1, 15 and 16, the Examiner admits that Ramasubramani does not teach that the certificate is a virus-free certificate. The Examiner contends that Parthasarathy at column 8, lines 35-47 teaches a virus-free certificate. However, this passage does not mention a virus-free certificate. In fact, Parthasarathy does not teach any virus-free certificate as noted in the above discussion. Therefore, the Examiner's contention is erroneous and the conclusion of obviousness is also erroneous.

The Examiner admits that Ramasubramani does not teach sending back in response to the virus-free request the received virus-free certificate. The Examiner contends that to do so would be obvious in view of Ramasubramani's teaching at column 7, lines 66 and 67. This passage distinguishes Ramasubramani's system from a traditional system by stating "unlike the tradition of physically storing the certificates in the local devices, the present invention maintains the certificates in a user account in the proxy server". That is, a purpose of Ramasubramani is not to store Ramasubramani's certificates in local stores, but rather in a proxy server. The modification to Ramasubramani proposed by the Examiner renders Ramasubramani unsatisfactory for such purpose. This is tantamount to a lack of motivation. See M.P.E.P., 2143.01 and cited cases. Moreover, the proposed modification changes Ramasubramani's

principle of operation (storing the certificates at the proxy server rather than locally). Accordingly, the teachings of Ramasubramani and the alleged tradition are not sufficient to render claims 1, 15 and 16 prima facie obvious. See 2143.01 and cited cases.

For the reason set forth above, it is submitted that the rejection of claims 1 and 13-16 under 35 U.S.C. 103(a) is erroneous and should be withdrawn.

The Office Action rejects claims 2-4 under 35 U.S.C 103(a) as unpatentable over Ramasubramani in view of Parthasarathy as applied to claim 1 and further in view of U.S Patent No. 6,574,663 to Bakshi et al., hereafter Bakshi.

Since claims 2-4 depend from claim 1, this rejection is erroneous for the same reason set forth in the discussion of claim 1.

For the reason set forth above, it is submitted that the rejection of claims 2-4 under 35 U.S.C. 103(a) is erroneous and should be withdrawn.

The Office Action rejects claims 5 and 7 under 35 U.S.C 103(a) as unpatentable over Ramasubramani in view of Parthasarathy as applied to claim 1 and further in view of U.S Patent No. 6,560,717 to Scott et al., hereafter Scott.

Since claims 5 and 7 depend from claim 1, this rejection is erroneous for the same reason set forth in the discussion of claim 1.

For the reason set forth above, it is submitted that the rejection of claims 5 and 7 under 35 U.S.C. 103(a) is erroneous and should be withdrawn.

The Office Action rejects claim 6 under 35 U.S.C 103(a) as unpatentable over Ramasubramani in view of Parthasarathy and Scott and further in view of U.S Patent No. 6,138162 to Pristriotto et al., hereafter Pristriotto.

Since claim 6 depends from claim 1, this rejection is erroneous for the same reason set forth in the discussion of claim 1.

For the reason set forth above, it is submitted that the rejection of claim 6 under 35 U.S.C. 103(a) is erroneous and should be withdrawn.

The Office Action rejects claim 8 under 35 U.S.C 103(a) as unpatentable over Ramasubramani in view of Parthasarathy, Scott and Pristriotto and further in view of U.S Patent No. 6,442,588 to Clark et al., hereafter Clark.

Since claim 8 depends from claim 1, this rejection is erroneous for the same reason set forth in the discussion of claim 1.

For the reason set forth above, it is submitted that the rejection of claim 8 under 35 U.S.C. 103(a) is erroneous and should be withdrawn.

The Office Action rejects claim 9 and 11 under 35 U.S.C 103(a) as unpatentable over Ramasubramani in view of Parthasarathy and Scott as applied to claim 5 and further in view of U.S Patent No. 6,078,955 to Konno et al., hereafter Konno.

Since claims 9 and 11 depend from claim 1, this rejection is erroneous for the same reason set forth in the discussion of claim 1.

For the reason set forth above, it is submitted that the rejection of claims 9 and 11 under 35 U.S.C. 103(a) is erroneous and should be withdrawn.

The Office Action rejects claim 10 and 12 under 35 U.S.C 103(a) as unpatentable over Ramasubramani in view of Parthasarathy, Scott and Konno as applied to claim 9 and further in view of Clark.

Since claims 10 and 12 depend from claim 1, this rejection is erroneous for the same reason set forth in the discussion of claim 1.

For the reason set forth above, it is submitted that the rejection of claims 10 and 12 under 35 U.S.C. 103(a) is erroneous and should be withdrawn.

The Office Action cites a number of patents that were not applied in the rejections of the claims. These patents have been reviewed, but are believed to be inapplicable to the claims.

It is respectfully requested for the reasons set forth above that the rejections under 35 U.S.C. 112 and 35 U.S.C. 103(a) be withdrawn, that claims 1-16 be allowed and that this application be passed to issue.

Respectfully Submitted,

Date: 6-17-04

Paul D. Greeley
Reg. No. 31,019
Attorney for Applicants
Ohlandt, Greeley, Ruggiero & Perle, L.L.P.
One Landmark Square, 10th Floor
Stamford, CT 06901-2682
(203) 327-4500